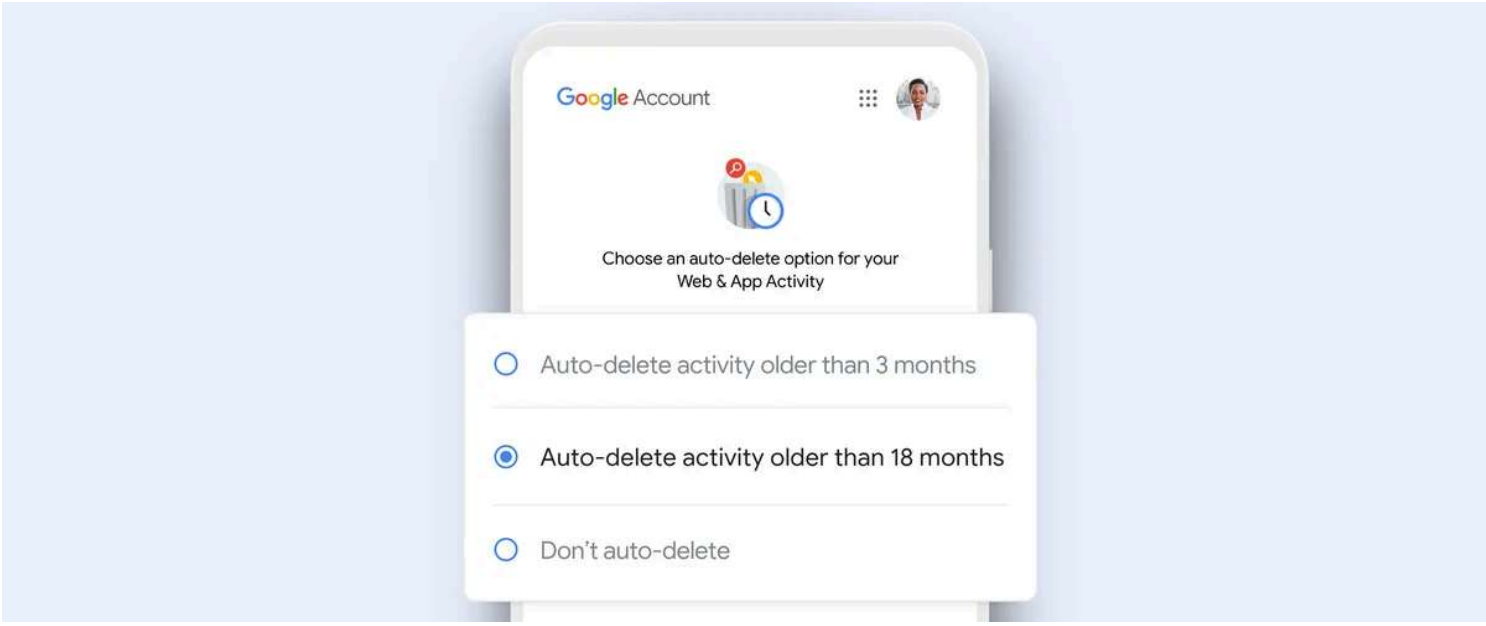
Exhibit 40

Keeping your private information private

Jun 24, 2020 · 5 min read

Share

Sundar Pichai
CEO of Google and Alphabet



Listen to article 7 minutes

Privacy is at the heart of everything we do, whether it's keeping Meet video calls secure, protecting you from security threats, or being the first major company to decide not to make general purpose facial

recognition commercially available and create clear AI Principles that prohibit use of our tools for surveillance.

As we design our products, we focus on three important principles: keeping your information safe, treating it responsibly, and putting you in control. Today, we are announcing privacy improvements to help do that, including changes to our data retention practices across our core products to keep less data by default.

Treating your information responsibly

We believe that products should keep your information for only as long as it's useful and helpful to you—whether that's being able to find your favorite destinations in Maps or getting recommendations for what to watch on YouTube.

That's why last year we introduced auto-delete controls, which give you the choice to have Google automatically and continuously delete your Location History, search, voice and YouTube activity data after 3 months or 18 months. We continue to challenge ourselves to do more with less, and today we're changing our data retention practices to make auto-delete the default for our core activity settings.

Here's how it works: Starting today, the first time you turn on Location History—which is off by default—your auto-delete option will be set to 18 months by default. Web & App Activity auto-delete will also default to 18 months for new accounts. This means your activity data will be automatically and continuously deleted after 18 months, rather than kept until you choose to delete it. You can always turn these settings off or change your auto-delete option.

If you've already had Location History and Web & App Activity turned on, we won't be changing your settings. But we will actively remind you about the auto-delete controls through in-product notifications and emails, so you can choose the auto-delete setting that works for you.

As we introduce default retention to more products, we're guided by the principle that products should keep information only for as long as it's useful to you. For example, we're bringing this to YouTube, where auto-delete will be set to 36 months by default if you create a new account or turn on your YouTube History for the first time. This improves upon current industry practice and ensures that YouTube can continue to make relevant entertainment recommendations based on what you've watched or listened to in the past—like letting you know if your favorite series has released another season, or when your favorite artist drops a new album. Current users can still choose the 3 or 18 months auto-delete option. Default retention periods will not apply to other products like Gmail, Drive and Photos, which are designed to safely store your personal content.

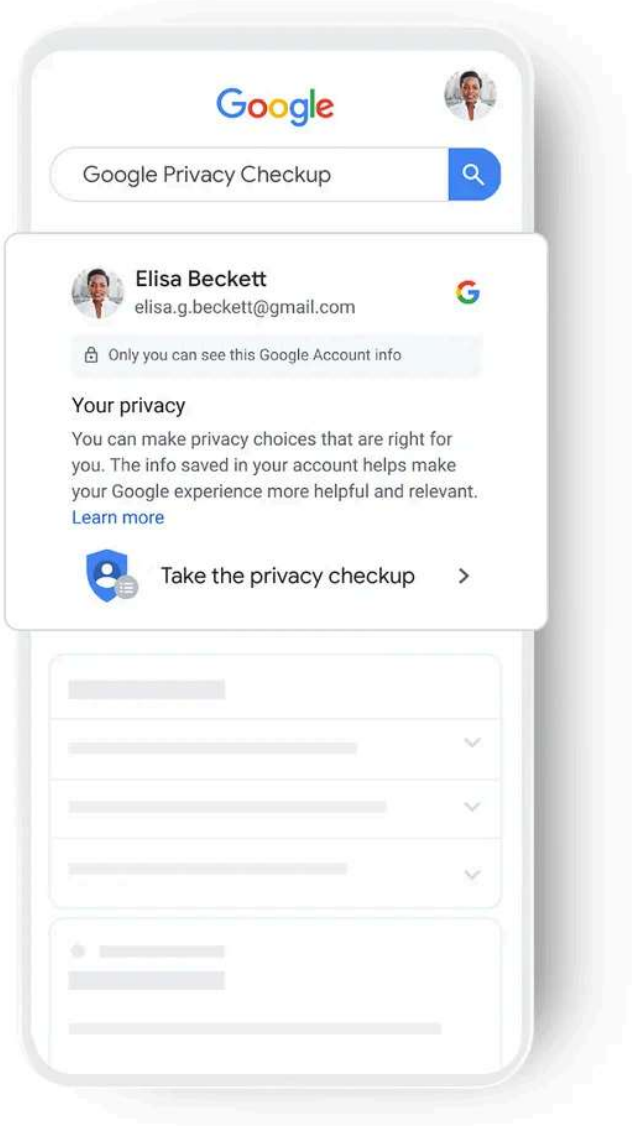
As always, we don't sell your information to anyone, and we don't use information in apps where you

primarily store personal content—such as Gmail, Drive, Calendar and Photos—for advertising purposes, period.

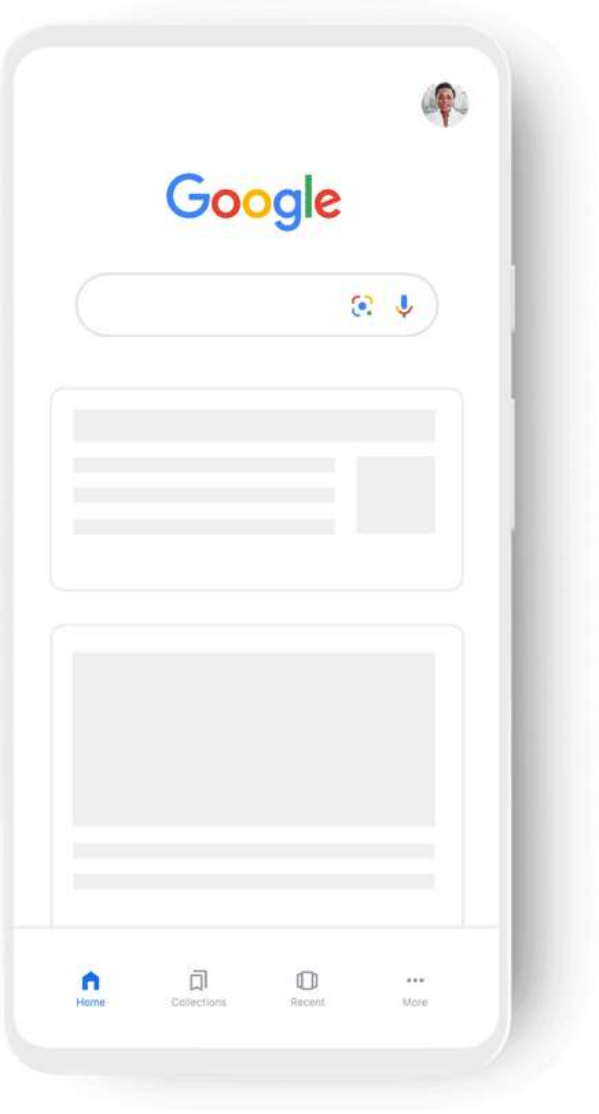
Control on your terms

Privacy is personal, which is why we're always working to give you control on your terms—whether that's helping you manage your settings with proactive tools in your Google Account, or making those settings easier to find in our products. Today we're announcing updates to many of our privacy tools.

- **Google Account controls directly from Search:** We're making it easier to access key Google Account controls from Search. Soon, when you're signed into your Google Account, you'll be able to search for things like "Google Privacy Checkup" and "Is my Google Account secure?" and a box only visible to you will show your privacy and security settings so you can easily review or adjust them.



- **Easier access to Incognito mode:** We're also making it easier to access Incognito mode in our most popular apps, by long-pressing on your profile picture in Search, Maps and YouTube. It's available today on the Google App for iOS, and coming soon to Android and other apps. We're also working to make it possible to stay in Incognito mode across Google apps, like Maps and YouTube, and will have more to share soon.



- **More proactive privacy controls:** Each year, more than 200 million people visit Privacy Checkup. We're adding proactive recommendations, including guided tips to help you manage your privacy settings.

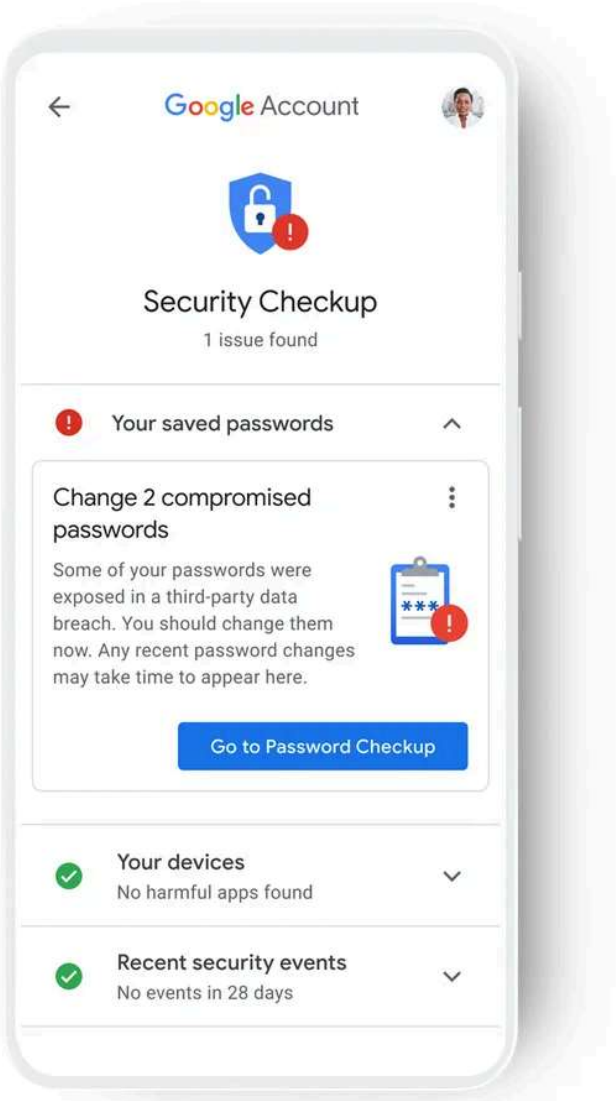
Proactively protecting your information

Protecting your privacy starts with the world's most advanced security. We provide automatic protections across all of our products, including Safe Browsing, which protects more than 4 billion devices from phishing

and malware every day, and Google Play Protect, which scans your apps before, during and after download to help keep your devices safe.

Five years ago we launched Security Checkup, an easy, one stop shop for securing your Google Account. In one click we'll give you a snapshot of your Account security and offer personalized recommendations to help keep your data safe. In the coming weeks, Password Checkup, our tool that checks if passwords saved to your Google Account have been compromised, will become a core part of Security Checkup.

More than 100 million people have used Password Checkup, and they've seen a 30 percent reduction in breached credentials—it's been an incredibly effective way of keeping people safe not just on Google, but across the web. Like the other elements of Security Checkup, we'll provide the information you need to secure any at-risk accounts, automatically. Now that it's been integrated into Google Account and Chrome, we'll be sunsetting the Password Checkup Chrome extension in the coming months.



Investing in privacy-preserving technologies

Being a responsible steward of your data means keeping it private. That's why we continue to make advances in privacy-preserving technologies and invest in thousands of privacy engineers to make our protections stronger across Google products. For example, differential privacy powers our COVID-19 Community Mobility Reports, which helps public health authorities combat COVID-19 by using location data in a privacy-preserving way. It's also used in Google Maps, so you can see how busy a restaurant is, in real time, without ever knowing who is at the restaurant. This year, in an industry first, we've used both differential privacy and federated learning, a technique we invented, to train the models that underpin Gboard. This successfully combines some of the most advanced methods to further protect your privacy.

Just as we open sourced Chromium to help make the open web better, we open sourced our differential privacy library to make it easier to build privacy into products across the industry. Now we're expanding it to new programming languages including Java and Go, and releasing additional tools to help developers use machine learning to enhance privacy protections.

Our work continues

As we make privacy and security advances in our own products, we continue to advocate for sensible data regulations around the world, including strong, comprehensive federal privacy legislation in the U.S. To help inform this work, we've published a regulatory framework based on privacy laws and models around the world, such as Europe's General Data Protection Regulation, and our own experience building privacy-first tools.

While policymakers continue their work, we will continue ours—by challenging ourselves to make helpful products with less data, and raise the bar on privacy for everyone.

POSTED IN:

Safety & Security